REMARKS

Applicants respectfully requests reconsideration and allowance of subject application. Claims 1-35 and 38-61 were pending at the time of the Action. Claims 3, 18, 28, 42, 51, and 59 are canceled. Claims 1, 4-5, 12, 16, 19-20, 26, 29-30, 31, 38, 40, 43-44, 49, 52-53, 58, and 60-61 are amended. Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 remain pending.

Applicants appreciate the Examiner taking the time to speak with their attorney regarding the Office Action.

CLAIM REJECTIONS UNDER 35 U.S.C. § 102

Claims 1-35, 38-46, 48-55, and 57-61 are rejected under 35 U.S.C. § 102 as being anticipated by Fox et al., "Security on the Move: Indirect Authentication Using Kerberos" (1996) (hereinafter "Fox"). Applicants respectfully traverse the rejection.

In the interest of reducing the complexity of the issues for the Examiner to consider in this response, the following discussion focuses on independent Claims 1, 12, 16, 26, 31, 38, 40, 49, and 58. The patentability of each remaining dependent claim is not necessarily separately addressed in detail. However, applicants' decision not to discuss the differences between the cited art and each dependent claim should not be considered as an admission that applicants concur with the Examiner's conclusion that these dependent claims are not patentable over the disclosure in the cited references. Similarly, applicants' decision not to discuss differences between the prior art and every claim element, or every comment made by the Examiner, should not be considered as an admission that applicants concur with the Examiner's interpretation and assertions regarding

those claims. Indeed, applicants believe that all of the dependent claims patentably distinguish over the references cited. Moreover, a specific traverse of the rejection of each dependent claim is not required, since dependent claims are patentable for at least the same reasons as the independent claims from which the dependent claims ultimately depend.

By way of introduction, the specification of the subject application addresses unconstrained forward target delegation. Generally, the user logon for a computer and the user authentication for network access control are two separate procedures. Nevertheless, to minimize the burden on a user in dealing with the different access control schemes, the user logon and the user authentication for network access are sometimes performed together. For example, in the case where the user authentication is implemented under the Kerberos protocol, when the user logs on the computer, the computer may also initiate a Kerberos authentication process. In the authentication process, the computer contacts a Kerberos Key Distribution Center (KDC) to first obtain a ticket-granting ticket (TGT) for the user. The computer can then use the TGT to obtain from the KDC, a session ticket for itself.

As networks have evolved, there has been a trend to have multiple tiers of server/service computers arranged to handle client computer requests. A simple example is a client computer making a request to a World Wide Web website via the Internet. Here, there may be a front-end web server that handles the formatting and associated business rules of the request, and a back-end server that manages a database for the website. For additional security, the web site may be configured such that an authentication protocol forwards (or delegates) credentials, such as, e.g., the user's TGT, and/or possibly other information from the front-end server

1 to a back-end server. This practice is becoming increasingly common in many

2 websites, and/or other multiple-tiered networks.

3 Thus, any server/computer in possession of the user's TGT and associated

4 authenticator can request tickets on behalf of the user/client from the KDC. This

5 capability is currently used to provide forwarded ticket delegation. Unfortunately,

6 such delegation to a server is essentially unconstrained for the life of the TGT.

7 Consequently, there is a need for improved methods and systems that support

8 delegation of authentication credentials in complex network configurations, but in

9 a more constrained manner.

10 Thus, as suggested in the subject application, authentication methods and

11 systems would benefit from a process of identifying a target service to which

12 access is sought on behalf of a client, and causing a server to request a new service

13 credential, for use by the server, from a trusted third-party. To accomplish this,

14 the server provides the trusted third-party with a credential authenticating the

15 server, information about the target service, and a service credential previously

16 obtained by the client, or by the server on behalf of the client. Here, the new

17 service credential is granted in the identity of the client rather than that of the

18 server.

19 Independent claims 1, 12, 16, 26, 31, 38, 40, 49, and 58, as amended, recite

20 a way of avoiding unconstrained delegation to a server. For example, claim 1, as

21 amended, is reproduced below:

22

23

24

25

1. (Currently Amended)   A method comprising:

identifying a target service to which access is sought on behalf of a client;

causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third-party, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and a service credential previously provided by the client to the server; and

requesting the trusted third-party to provide the server with a new service credential granted in the name of the client rather than the server such that the new service credential authorizes the server to access the service on behalf of the client.

Applicants submit that claim 1 as amended, as well as other the independent claims as amended, are not anticipated by Fox.

Fox describes a system for allowing portable devices to securely access resources on a network through the use of proxies. The title of the reference, "Security on the Move: Indirect Authentication Using Kerberos," aptly describes its content. Fox is directed to network data security when portable devices, such as personal digital assistants (PDAs), are used to access a network. Moreover, as described in Fox, because such portable devices have comparatively limited capabilities, network access and authentication are indirect in that both are handled through the use of a "proxy" executing on a more robust system:

"PDA's and personal communications devices are in every respect very modest compared to laptops: they have smaller screens, less memory, less powerful processors, stripped-down operating systems and programmatic API's, and weak (typically wireless) communication. To compensate for these differences, **the strategy of mediating access via *proxies* – computation inserted between the client and server – is becoming pervasive.**"

(Fox, page 155, column 2, paragraph 2; bold emphasis added; italics original).

Thus, for "enabling secure access to **proxied** services," Fox describes "Charon, a proxied implementation for *indirect authentication* and secure communications with personal mobile devices," where Fox defines "indirect" as when "most of the computational resources needed to conduct the Kerberos protocol and establish a secure channel are located at a *proxy*, a process running on a desktop workstation in the wired infrastructure." (Fox, page 155, column 2, paragraph 5; bold emphasis added; italics original).

More specifically, Fox's Charon system describes itself as a two-phase process. A first phase is a handshaking phase which, as acknowledged by Fox, itself includes two steps. In a first step, the portable client device establishes a secure channel to the proxy. (Fox, page 157, column 1, paragraph 2). Then, in a second step, the portable client uses the proxy as "an intelligent router" to obtain a "ticket granting ticket" or "TGT" by which the proxy then is able to seek tickets to access network services. (Fox, page 157, column 1, paragraph 3).

A second phase is a service access phase through which the proxy, using the TGT issued on behalf of the client, accesses a "ticket granting service" or "TGS," to get a ticket that authenticates the authority of the proxy to access a network service on behalf of the client. (Fox, page 157, column 1, paragraph 4). The proxy then uses the ticket to access a network service. (Fox, page 157,

1   column 2, paragraph 2). Therefore, the second phase also is a two-step process

2   wherein the proxy obtains a ticket from a TGS that the proxy uses the ticket to

3   access the service.

4   In sum, to offload processing responsibilities from a portable device of

5   limited capabilities, Fox discloses establishing a proxy on a more robust network

6   device that, in effect, participates in the network for the portable device. Thus, the

7   proxy obtains a ticket granting ticket to be able to request access to network

8   resources, and interact both with a ticket granting service and services. The proxy

9   directly engages the ticket granting service to secure authentication to access a

10   service, and then the proxy uses that ticket to directly request access to a server or

11   other network service.

12   Respectfully, Fox fails to disclose each of the elements recited in the

13   claims, and thus does not anticipate the claims. Applicants have amended the

14   independent claims to further clarify the distinctions between them and Fox.

15

16   ### CLAIMS 1, 3-5, 12, 16, 18-20, 26, 28-30, 31, 33, AND 25

17   Applicants assert that these claims are not anticipated by Fox for at least

18   three reasons. The Office Action collectively rejects independent claims 1, 12, 16,

19   26, and 31, and claims depending therefrom based on comparing the reference

20   with the elements of claim 12 as a representative claim. Applicants therefore

21   respond to the rejections in the same manner.

22   First, Fox neither teaches nor suggests "identifying a target service to which

23   access is sought on behalf of a client." The Office Action cites Fox for reciting

24   that its system includes a "service access phase, in which the proxy accesses

25

Kerberized services on the client's behalf." Nonetheless, even once the service

phase is accessed, Fox does not disclose identifying a target service.

Second, Fox neither teaches nor suggests causing a server to request access

to a target service. Again, Fox discloses using a proxy, acting in the position of its

client, to actively seek tickets and actively use the tickets to access services. For

convenience, applicants reproduce portions of Fox and the elements of the claims

to which they were equated in the Office Action. Specifically, the Office Action

equated:

> "identifying a target service to which access is sought on behalf of a client; and causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third party,"

as recited in Claim 12, with Fox's recitation that:

> "Charon's interaction consists of two distinct phases: the handshake phase, in which the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it, and the service access phase, *in which the proxy accesses Kerberized services on the client's behalf.* The Charon protocol module on the proxy and the Charon client-side software are responsible for the flow of control during both phases."

(Fox, page 157, column 1, paragraph 2; emphasis added).

Thus, the claim recites "causing a server . . . to request access to the target

service," while in Fox, the proxy "accesses services on the client's behalf."

According to Fox, network services are requested by a proxy and not by the client

itself. However, the proxy is an intermediary of the client through which the client

accesses services. In other words, as quoted in the Office Action, "the client uses

the proxy as an intelligent router." (Fox, page 157, column 1, paragraph 3).

Clearly, neither Fox's proxy nor its client causes a server to request access to the

target service. Thus, because Fox's proxy accesses services rather than cause a

server to request access to such services, Fox neither teaches nor discloses the claimed elements.

Second, neither the portions of Fox cited in the Office Action nor any other disclosure made by Fox includes a description of how a target service that does not reside on a server accessed by the client might be accessed. Thus, while elements of the claims quoted recite "causing a server . . . to request access to the target service," Fox nowhere discloses "a target service," let alone causing a server to request access to such a client service.

Third, the independent claims are amended to further clarify the distinctions between the claims and the cited reference. For example, claim 1 is amended to recite:

> "requesting the trusted third-party to provide the server with
> a new service credential granted in the name of the client rather than
> the server such that the new service credential authorizes the server
> to access the service on behalf of the client."

Respectfully, nothing in the portions of Fox cited in the Office Action or anywhere else in the reference does Fox describe issuance of a new service credential to a server in the name of the client rather than the server.

In sum, because Fox fails to teach or suggest the elements recited in the claims, applicants request that the rejection be withdrawn from independent claims 1, 12, 16, 26, and 31. Moreover, because dependent claims are patentable for at least the same reasons as the claims from which they depend, and add additional limitations to those claims, applicants request that the rejection similarly be withdrawn from claims 2, 4-11, 13-15, 17, 19-25, 27, 29-30, 33, and 35.

CLAIMS 38 AND 39

Applicants assert that claims 38 and 39 are not anticipated by Fox for at least three reasons. First, Fox neither teaches nor discloses "separately authenticating a server and a client; providing the client with a client ticket granting ticket and a service ticket for use with the server" as recited in claim 38. The Office Action equates this element with Fox's statement that "the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it." (Fox, page 157, column 1, paragraph 2). However, nothing in Fox, within the cited passage or elsewhere in the reference, discloses authenticating a server. Furthermore, nothing in Fox teaches or suggests separately authenticating a server and a client, nor does Fox teach or suggest separately authenticating its client and proxy. In addition, there is no mention of a service ticket being provided for use with a server. Fox's description of client authentication to a proxy fails to teach or suggest these elements.

Second, Fox neither suggests nor discloses "providing the server with a new service ticket for use by the server for use with a new service without requiring the server to have access to the client ticket granting ticket." Fox discloses how a proxy acts on behalf of a client and handles all client requests and authentication: "the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy. From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client." (Fox, p. 157, column 1, paragraph 3). Thus, according to Fox, all requests are still handled by the client through this "intelligent router" proxy. Fox does not describe providing any ticket to the server, let alone "providing the server with a new service ticket for use by the server without the client requiring the server to have access to the client ticket

28

granting ticket" as recited in claim 38. Thus, Fox fails to teach or suggest the server ticket or the new service ticket.

Third, claim 38 is amended to further clarify the distinctions between claim 38 and the cited reference. Specifically, claim 38 is amended to recite that the new service ticket "provided in an identity of the client rather than an identity of the server." Fox neither teaches nor suggests a server being provided with a service ticket in an identity of the client, and thus fails to anticipate claim 38.

In sum, because Fox fails to teach or suggest the elements recited in the claim 38, applicants request that the rejection be withdrawn. Moreover, because a dependent claim is patentable for at least the same reasons as the claim from which it depends, and adds additional limitations to the claim, applicants request that the rejection similarly be withdrawn from claim 39.

CLAIMS 40, 48, 49, 57, AND 58

Applicants assert that independent claims 40, 49, and 58, and claims depending therefrom, are not anticipated by Fox for at least four reasons. The Office Action collectively rejects independent claims 40, 49, and 58, and claims depending therefrom based on comparing the reference with the elements of claim 40 as a representative claim. Applicants therefore respond to the rejections in the same manner.

First, Fox neither teaches nor suggests "identifying a target service to which access is sought on behalf of a client." The Office Action cites Fox for reciting that its system includes a "service access phase, in which the proxy accesses Kerberized services on the client's behalf." Nonetheless, even once the service phase is accessed, Fox does not disclose identifying a target service.

Second, Fox neither teaches nor suggests "causing a server . . . to request a service credential." As previously described, Fox describes how the client uses a proxy as an intelligent router to obtain services. However, as also previously described, Fox nowhere discloses causing a server to request a service credential.

Third, Fox neither teaches nor suggests "causing the server to request a new service credential, for use by the server and the target service." Again, not only does Fox not describe a target service or causing a server to request a service credential, but Fox fails to describe that a server might be caused to request a new service credential for use by the server and a target service.

Fourth, claim 40 is amended to further clarify that the new service credential is requested "in an identity of the client rather than an identity of the server." Fox neither teaches nor suggests a server being provided with a service credential in an identity of the client, and thus fails to anticipate the claim.

In sum, because Fox fails to teach or suggest the elements recited in the claims 40, 49, and 58, applicants request that the rejection be withdrawn. Moreover, because dependent claims 41, 43-48, 50, 52-57, and 60-61 are patentable for at least the same reasons as the claims from which they depend, and add additional limitations to those claims, applicants request that the rejection similarly be withdrawn from these claims.

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

Claims 47 and 56 are rejected under 35 U.S.C. § 103(a) as being obvious over Fox in view of Freier et al., "The SSL Protocol Version 3.0" (November 18, 1996). Claims 47 and 56 depend from claims 40 and 59, respectively. Because dependent claims 47 and 56 are patentable for at least the same reasons as the
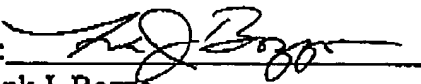
claims from which they depend, and add additional limitations to those claims, applicants request that the rejection similarly be withdrawn from claims 47 and 56.

CONCLUSION

Claims 1-2, 4-17, 19-27, 29-36, 38-41, 43-50, 52-58, and 60-61 are in condition for allowance. Applicant respectfully requests entry of the amendment, and reconsideration and prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, the Examiner is requested to contact the undersigned attorney to resolve the issue.

Respectfully Submitted,

Dated: *November 23, 2005*

By: _____
Frank J. Bozzo
Reg. No. 36,756
(206) 315-4001